AT-S63 Version 2.2.0 Management Software for the AT-9400 Series Layer 2+ and Basic Layer 3 Gigabit Ethernet Switches Software Release Notes

Please read this document before you begin to use the management software.

Supported Platforms

The AT-S63 Version 2.2.0 management software is supported on the following AT-9400 Series Gigabit Ethernet switches:

Layer 2+ Models	AT-9408LC/SP (AC)
	AT-9424T/GB (AC)
	AT-9424T/SP (AC)
	AT-9424T/GB-80 (DC)
	AT-9424T/SP-80 (DC)
Basic Layer 3 Models	AT-9424Ts (AC)
	AT-9424Ts/XP (AC)
	AT-9448T/SP (AC)
	AT-9448Ts/XP (AC)

Note:
The Layer 2+ and Basic Layer 3 models support all the same features, except for Internet Protocol version 4 packet routing and MAC address-based VLANs, which are only supported on the Basic Layer 3 switches.

This release supports the following redundant power supply on the AC models:

- AT-RPS3204

For a list of supported GBIC, SFP, and XFP modules, contact your Allied Telesis sales representative.

Product Documentation

For hardware installation instructions, refer to the following guide:

- *AT-9400 Series Gigabit Ethernet Switches Installation Guide* (PN 613-000357-00)

For management instructions, refer to the following guides:

- *AT-S63 Management Software Menus Interface User's Guide* (PN 613-50570-00)
- *AT-S63 Management Software Web Browser Interface User's Guide* (PN 613-50592-00)
- *AT-S63 Management Software Command Line Interface User's Guide* (PN 613-50571-00)

All documents are available from the Allied Telesis web site at **www.alliedtelesis.com**.

Caution:
The software described in the documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a "retail encryption item" in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesis sales representative for current information on this product's export status.

Note:
The Public Key Infrastructure (PKI), Secure Sockets Layer (SSL), and Secure Shell (SSH) encryption features, offered separately prior to version 2.0.0, are now standard components of the AT-S63 management software.

Switch Models and Management Software Versions

The following table lists the models in the AT-9400 Series and the version of the AT-S63 Management Software where each model was initially supported. You can refer to the table to determine whether a version of the management software supports a particular model in the event you load an older version onto a unit. For example, support for the AT-9424Ts switch, the newest model in the series, was introduced in version 2.1.1. Any attempt to load an earlier version of the software onto that model will be unsuccessful.

Model	AT-S63 Management Software Version
AT-9424T/GB	1.0.0
AT-9424T/SP	1.0.0
AT-9408LC/SP	1.1.0
AT-9448Ts/XP	1.3.0
AT-9448T/SP	2.0.0
AT-9424Ts/XP	2.0.0
AT-9424Ts	2.1.1

What's New in Version 2.2.0

No new features.

Known Issues

- Maximum bandwidth parameter in QoS policies. A QoS policy that has multiple traffic classes with different values for the maximum bandwidth parameter uses the lowest specified maximum bandwidth value for traffic flows that match more than one traffic class. (4137)
- 802.1x "control direction" feature. The "control direction" feature of 802.1x port-based network access control is nonfunctional for IGMP multicast packets when IGMP snooping is enabled on the switch. This feature is suppose to control the forwarding of multicast and broadcast packets by an authenticator port in the unauthorized state. When IGMP snooping is enabled, an authenticator port always forwards IGMP multicast packets, regardless of the status of the "control direction" feature. (4206)
- VLAN ingress filtering. Untagged packets may periodically cross VLAN boundaries and be retransmitted as tagged packets from the switch's ports when the VLAN ingress filtering feature is disabled. The VLAN ingress filtering feature controls whether tagged packets are filtered on the ingress or egress ports for the packets. Untagged packets are not suppose to be affected by this feature and should never cross VLAN boundaries. (4455)
- LACP trunks. When a link is lost and later reestablished on an active port in an LACP trunk, the switch may take upwards of 30 seconds before it begins to forward traffic again over the reestablished link. (4514)
- SET IP ARP Command. The format of this command in AT-S63 versions 2.0.0 was as follows: (4521)

  `set ip arp arp=`*`ipaddress`* `[interface=`*`interface`*`] [port=`*`port`*`] [ethernet=`*`macaddress`*`]`

  In version 2.1.0 and all future versions, the format will not include the first "arp":

  `set ip arp=`*`ipaddress`* `[interface=`*`interface`*`] [port=`*`port`*`] [ethernet=`*`macaddress`*`]`
- Tagged ports and LACP aggregators. An LACP aggregator can not contain tagged ports, but the management software does allow it if you create the aggregator first and the VLANs afterwards. The performance of an aggregate trunk in an aggregator with tagged ports may be unpredictable. To avoid this issue, you should verify that the ports of an aggregator are not tagged ports of any VLAN on the switch. (4585)
- Static port trunks and dynamic LACP port trunks. The management software allows you to create up to seven static and dynamic port trunks on the switch, though the actual maximum number is six. The performance of one or more of the trunks may be unpredictable when a switch has seven port trunks. (4630)
- Guest VLAN. The Guest VLAN feature of 802.1x port-based network access control is nonfunctional. An authenticator port assigned a Guest VLAN will remain in the unauthorized state and will not transition to the VLAN when an unauthorized individual accesses the port. (4641)
- Switch's MAC address and IP multicast packets. The switch might stop forwarding network traffic if it receives an IP multicast packet that has its MAC address as the destination address and a TCP header in the payload. To resolve this problem, you must reset the unit. (4722)

- MAC address-based VLANS. The list of switches that support this feature is incorrect in the version 2.0.0 documentation. This feature is supported on the AT-9424Ts, AT-9424Ts/XP, AT-9448T/SP, and AT-9448Ts/XP switches, but not on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches.

Resolved Issue

- Filter-based features. IGMP and MLD snooping did not work on the AT-9424Ts and AT-9424Ts/XP switches. This issue has been resolved. (4199)

Operational Notes

- Classifier criteria on AT-9424Ts and AT-9424Ts/XP switches. Access control lists and Quality of Service policies on these switches cannot filter on the following combinations of classifier criteria:
  - VLAN ID with source or destination IP address.
  - Protocol with source or destination IP address

  This rule applies whether the criteria are in the same classifier or different classifiers of an access control list or Quality of Service policy.
- Spanning tree and LACP trunks. A spanning tree protocol on a switch with two or more LACP trunks uses the trunk ID number to select a trunk to place in the blocking state if the trunks form a network loop. The trunk ID number is automatically assigned by the management software when an aggregator is created, starting with 0 (zero) and incremented by 1 with each new aggregator. The lower the trunk ID number, the higher the priority. For instance, if a switch has two LACP trunks, a spanning tree protocol will block the ports of the trunk with the higher ID number (lower priority) should it determine that the trunks form a loop. (4261)
- Denial of Service defense mechanisms. The operation of a Denial or Service defense mechanism on the switch might be unpredictable when a defense is assigned to more than one port or when more than one defense is assigned to the same port. This issue can be avoided by not assigning a defense mechanism to more than one port or more than one defense mechanism to a port. This issue is limited to the AT-9424Ts and AT-9424Ts/XP switches. (4196)
- QoS policies and unicast and multicast addresses. The filtering properties of a QoS policy are designed for known unicast addresses. The behavior of a policy may be unpredictable if it filters on unknown unicast addresses or known or unknown multicast addresses. (3196)
- Enhanced stacking and slave switches. The AT-S63 Version 2.0.0 Management Software User Guides incorrectly state that slave switches in an enhanced stack do not need a routing interface on the common VLAN that interconnects them with the master switch. Actually, a routing interface is required in the common VLAN of a slave switch, but it does not have to be designated as the local interface, except on the master switch. The only exception to this rule is if you use the Default_VLAN (VID 1) as the common VLAN, in which case the common VLAN on a slave switch does not need a routing interface. (4517)
- Lowest numbered port in an LACP aggregator. You cannot delete the lowest numbered port from an LACP aggregator, referred to as the base port, or add a port to an aggregator that is below the base port. The OperKey parameter for the ports in an aggregator is based on the lowest numbered port and cannot be changed after the aggregator is created. For example, if you create an aggregator of ports 10 to 15 on a switch, you cannot later delete port 10 from the aggregator or add a port less than port 10. You must recreate the aggregator if you need to change the base port. (4369)

- Saving a configuration. The management software on the switch may experience a problem if you save configuration changes in rapid succession. To avoid this issue, you should wait for the Fault LED on the front panel of the switch to go off after you save a configuration change and before you save another configuration change. If you are in a different location from the switch and cannot view the Fault LED, you should wait 30 to 45 seconds between your save commands. (2683)
- Multiple VLAN modes and IPv4 packet routing. The 802.1Q-compliant and non-802.1Q-compliant multiple VLAN modes do not support IPv4 packet routing. You cannot configure routing interfaces when the switch is running in either of these VLAN modes, and all existing routing interfaces, with the exception of the local interface, are deleted when one of these VLAN modes is activated. To assign an IP address to a switch running one of these VLAN modes, you must create one routing interface and designate it as the local interface while the switch is running in the user-configured VLAN mode, and afterwards change the switch's VLAN mode to 802.1Q-compliant or non-802.1Q-compliant. The local interface is automatically moved to the VLAN on port 1 of the switch. (3806)
- Switch to switch upload of a configuration file. The *AT-S63 Management Software User Guides* state that the configuration file on a master switch retains its routing interface commands when uploaded to a slave switch. This is incorrect when the file is the master switch's active configuration file. All routing interface commands are removed from the master switch's active configuration file when it is uploaded to a slave switch to prevent an IP address conflict on the units. However, the routing interface definitions in the file are retained when you upload any other configuration file from a master switch to a slave switch. (4272)
- Telnet management session. Changing the VLAN mode of a switch (e.g., from the user-configured VLAN mode to a multiple VLAN mode) from a remote Telnet management session may end your management session. To continue managing the switch, you must reestablish the management session (3806)
- SNMPv3 management. The enhanced stacking feature is not supported from SNMPv3. (4065)
- AtiStkSwVlanConfigEntry MIB table. The response time of the management firmware on the switch will slow if you have more than one instance of the AtiStkSwVlanConfigEntry MIB table open at a time. (2231)
- Compact flash card. Removing a compact flash card from the switch while the management software is writing a file to it may cause the switch to stop responding to management commands and forwarding network packets. To avoid this issue, never remove a compact flash card from the switch while the Fault LED on the front panel is on. Wait for the Fault LED to turn off before removing the card.(4253)
- LACP priority value and the event log. A change to a switch's LACP priority value is registered in the event log with a message that reflects the current status of LACP, rather than the change to the priority value. The log message is either "lacp:enabled" or "lacp:disabled." (3345)
- MAC address-based VLANs and static trunks. The documentation states that the ports of a MAC address-based VLAN form a community and that the assignment of a MAC address to one port in a VLAN is equivalent to assigning it to all ports. This is true except in the case where the ports of a MAC address-based VLAN encompass a static port trunk, in which case the same MAC addresses must be assigned to all the ports in the trunk. (3249)
- File upload or download. The switch's response to management instructions may be slow while it uploads or downloads a file to the file system.

- Flow control and back pressure. Flow control and back pressure are operational *among* devices connected to ports 1 through 12 or ports 13 through 24 on the AT-9424T/GB and AT-9424T/SP switches, but not *between* devices connected to ports 1 through 12 and 13 through 24. (1321, 1322)
- Reserved multicast traffic and port mirroring. The destination port of a port mirror may transmit duplicates of some reserved multicast traffic, such as STP BPDUs and other control packets. The duplication results from the destination mirror port transmitting both the reserved multicast traffic it receives from flooded multicast traffic and the same multicast traffic from the mirrored ports. (3055)
- Fiber optic port configuration display. The Auto-Negotiation, speed, and duplex mode settings in the menus interface for ports 23 and 24 on the AT-9424T/GB and AT-9424T/SP switches always reflect the settings of the corresponding twisted pair ports 23R and 24R. They do not reflect the current settings of an active GBIC or SFP fiber optic port. (3047)
- GVRP compatibility. There may be some compatibility issues with GVRP and other switches. To work around this situation, change the Join and Leave time from the defaults to: Join Timer = 60 and Leave Timer = 120.
- Port configuration. The speed, duplex mode, and MDI/MDIX settings of a 10/100/1000Base-T twisted pair port are changed as a unit when configuring multiple ports simultaneously. The settings of the lowest numbered port being configured are automatically copied to the other ports. For example, if you configure ports 1 to 4 simultaneously and change the MDI/MDIX setting, the speed and duplex mode settings of port 1, along with the new MDI/MDIX setting, are copied to ports 2 to 4. (1262)
- Static and LACP port trunks and load distribution methods. The following load distribution methods for static and LACP port trunks are nonfunctional: source IP address, destination IP address, and source/destination IP addresses. The switch uses source MAC address, destination MAC address, or source/destination MAC addresses, respectively, if a nonfunctional load distribution method is selected.
- Jumbo frames. Frame loss may occur when jumbo frames are being transferred on more than two ports. (1412, 2783, 2792)
- Xmodem downloads. The switch does not respond to echo requests or send or respond to STP BPDU packets during an Xmodem download of system software. Also, echo request responses are slowed when there is a TFTP transfer in progress and the echo requests are received within the same port group as the TFTP server. (1663, 1582)
- SFP and GBIC ports. The switch considers the fiber optic port on an optional SFP or GBIC module in the AT-9424T/GB and AT-9424T/SP switches as active if it is receiving a signal, even if the port has not established a valid link with the remote node. If an optional fiber optic port loses or is unable to establish a link but is receiving a signal, it remains as the active port and the switch does not activate the corresponding twisted pair port 23R or 24R. (2850)
- Web browser interface. The web browser interface works best with Microsoft Internet Explorer version 6.0 and above. Results using other versions or other web browser applications may vary.
- Configuration files. Do not use Microsoft's NotePad to edit or view a configuration file. Some versions of NotePad may add formatting codes to the file. Use WordPad instead or some other text editor that will not add formatting codes to the file. When saving the file, do not change the ".cfg" extension in the filename or save the file with formatting codes.

- Enhanced stacking. The IP address 172.16.16.16 is reserved for the enhanced stacking feature. Do not assign this address to any device in the same subnet as an enhanced stack.
- Login password. The maximum length of a login password is 16 alphanumeric characters for manager accounts created through the RADIUS and TACACS+ authentication protocols and supplicant accounts for 802.1x port-based network access control. Passwords that exceed this limit will not work.
- TACACS+. The TACACS+ client software on the switch supports Password Protection Protocol (PAP), but not Challenge Handshake Authentication Protocol (CHAP) or AppleTalk Remote Access Protocol (ARAP). (1078)
- Port settings. A port, when removed from a port trunk, retains its settings as a member of the trunk. The parameter settings (e.g., speed and duplex mode) are not returned to the default values. (2144)
- MAC addresses. You must move the cursor manually from field to field when entering an IP or MAC address in the web browser interface. The cursor does not move automatically as you enter the parts of an address. (1699, 2123)
- SNTP. The SNTP client software on the switch sends a Transmit Time Stamp with a value NULL when synchronizing with a Network Time Protocol server. This does not affect the operation of the SNTP client software. (1676)
- IGMP. The switch, when configured for IGMP, will not register tagged IGMP queries in the IGMP routers list if ingress filtering is disabled. (1493)
- SFP modules and the AT-9408LC/SP switch. Be sure to disconnect the fiber optic cable from an SFP module in an AT-9408LC/SP switch before removing the module. The L/A LED for the slot may remain on if you remove an SFP module while it has a link to an end node. This problem does not affect the operation of the switch or the SFP slot. The L/A LED goes off the next time you install an SFP module in the slot.

Features History

Version 2.1.1:

- The number of cooling fans in the AT-9424Ts switch was reduced from four to three. The AT-S63 management software was updated to reflect the change.

Version 2.1.0:

- Multiple IPv4 routes with Equal Cost Multi-path (ECMP). The switch now supports ECMP and multiple routes to the same remote destination. For further information, refer to "Changes to Internet Protocol Version 4 (IPv4) Routing in Version 2.1.0," later in these software release notes. For background information on the IPv4 packet routing feature and descriptions of the command line commands, refer to Chapter 32, "Internet Protocol Version 4 Packet Routing," in the latest version of the *AT-S63 Management Software Command Line Interface User's Guide*.
- Variable length subnet masks for IPv4 routing. Previously, a byte in a subnet mask for a route in the IPv4 routing table had to be 0 or 255. The switch now accepts masks of variable length. For further information, refer to "Changes to Internet Protocol Version 4 (IPv4) Routing in Version 2.1.0," later in these software release notes.
- Multiple default routes. In the previous version, there could be only one default route for the IPv4 packet routing feature and the route was not propagated by RIP. In this version, the routing table can store and propagate multiple static and dynamic default routes. For further information, refer to "Changes to Internet Protocol Version 4 (IPv4) Routing in Version 2.1.0," later in these software release notes.
- 802.1x authenticator ports. The maximum number of supplicants that can be logged on to an authenticator port running in the multiple operating mode has been increased from 20 clients to 320 clients. However, the maximum number of logged on clients per switch remains the same at 480 clients. (4186)

Note:
The IPv4 routing feature is not supported on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches. These switches support only one routing interface to assign the device an IP address. For further information, refer to the latest version of the *AT-S63 Management Software Command Line Interface User's Guide*,

Version 2.0.0:

- Internet Protocol Version 4 (IPv4) packet routing. The AT-9400 Series switch features IPv4 packet routing with routing interfaces, static routes, and the Routing Information Protocol versions 1 and 2. For background information, refer to Chapter 32, "Internet Protocol Version 4 Packet Routing," in the latest version of the *AT-S63 Management Software Command Line Interface User's Guide*.
- Secure Shell (SSH) protocol server. The security of the SSH server on the switch has been enhanced to prevent unauthorized management access to the switch. The AT-S63 management software now disables the SSH server, logs an event in the event logs with the client's IP address, and sends an SNMP trap if it detects fifty consecutive failed login attempts from an SSH client.
- Class of Service and Queue 7. The range of the maximum number of transmitted packets for the CoS weighted round robin scheduling method has been changed for Queue 7 (Q7). The range was 1 to 15; the new range is 0 (zero) to 15. Setting Q7 to 0 gives its packets priority

over packets in the other queues. No packets are transmitted from the lower priority queues so long as there are packets in Q7. (3803)

- Temperature threshold alert. The temperature threshold alert feature now has two levels. An ambient temperature of 55° to 60° Celsius for ten minutes activates the first level. The switch sends a SNMP trap and enters a warning event message in the event logs. The second level, activated if the ambient temperature exceeds 60° Celsius for five minutes, sends another SNMP trap, logs an error event message, and activates the Fault LED on the front panel.

Version 1.3.0:

- Added the following new features to 802.1x port-based network access control:
  - Guest VLANs
  - VLAN Assignment and Secure VLAN features for supporting dynamic VLAN assignments with supplicant accounts.
  - MAC address-based authentication as an alternative to 802.1x username and password authentication.
- Simplified the menu interface for managing the access control entries in the Management ACL.

Version 1.2.0:

- MLD snooping for MLDv1 and MLDv2.
- 802.1x port-based network access control supports up to 20 supplicants simultaneously on an authenticator port.
- Quality of Service has the following new actions:
  - Set Type of Service (ToS)
  - Move Type of Service to 802.1p Priority
  - Move 802.1p Priority to Type of Service
  - Send to Mirror Port
- The command line interface has new command parameters for displaying and deleting specific types of MAC addresses from the MAC address table.

Version 1.1.0:

- LACP (802.3ad)
- Policy-based QoS (Classifiers, Flow Groups, Traffic Classes, and Policies)
- Flash memory operations
- Access Control Lists (ACLs)
- Syslog support
- Password reset
- Redundant power supply information
- IGMP v3 Snooping
- New web browser interface procedures

Version 1.0.0:

- Auto-Negotiation (IEEE 803.3u-compliant) for speed and duplex mode
- Auto and manual MDI/MDI-X
- Flow control (IEEE 802.3x and 802.3z-compliant)
- Head of line blocking prevention
- Unicast, multicast, and broadcast rate control
- Port mirroring
- Port trunking (IEEE 802.3ad) (static link aggregation, non LACP)
- Port security
- Port statistics (RMON)
- 1000 static MAC addresses, 16K dynamic MAC addresses, 256 static multicast addresses, 255 dynamic MAC addresses (snooping)
- Spanning Tree Protocol (IEEE 802.1D)
- Rapid Spanning Tree Protocol (IEEE 802.1w)
- Multiple Spanning Tree Protocol (IEEE 802.1s)
- Virtual LANs (IEEE 802.1Q)
- Protected ports VLANs
- Ingress filtering
- GARP VLAN Registration Protocol (GVRP)-based dynamic VLANs
- Secure Sockets Layer (SSL) Protocol (not included in AT-S63 NE)
- Secure Shell (SSH) Protocol (not included in AT-S63 NE)
- Public Key Infrastructure (PKI) Certificates (not included in AT-S63 NE)
- Static and dynamic system time (SNTP client)
- Management VLAN
- Multiple VLAN modes
- Event log
- Enhanced stacking (for management)
- IGMP Snooping (RFC 2236)
- Class of Service (IEEE 802.1p-compliant)
- Queuing - map 802.1p to CoS queue to prioritize traffic at egress
- Strict priority and weighted round robin priority scheduling
- RRP Snooping
- File system
- SNMPv1, SNMPv2c and SNMPv3 management
- CLI-based configuration file
- Denial of Service detection
- 802.1x Port-based Network Access Control
- RADIUS accounting

- Menus, CLI, web, and SNMP interfaces
- Password protected management access
- Management access control list
- Local authentication
- RADIUS and TACACS+ authentication protocols
- Xmodem and TFTP downloads and uploads, HTTP and enhanced stacking
- Static IP configuration
- BOOTP and DHCP
- Fan and temperature information
- CPU, Flash, and RAM information
- Power supply, redundant power supply, and transceiver information

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **www.alliedtelesis.com/support/kb.aspx**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support section of the Allied Telesis web site: **www.alliedtelesis.com**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. For instructions on how to obtain an RMA number, go to the Support section on our web site at **www.alliedtelesis.com**.

For Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at **www.alliedtelesis.com**.

Obtaining Management Software Updates

New releases of management software for our managed products are available from the following Internet sites:

- Allied Telesis web site: **www.alliedtelesis.com**
- Allied Telesis FTP server: **ftp://ftp.alliedtelesis.com**

If the FTP server prompts you to log on, enter "anonymous" as the user name and your email address as the password.